UNIVERSITAS GADJAH MADA
IMPLEMENTASI OSSIM DAN SPLUNK UNTUK MONITORING DAN ANALISA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
EMITA ARIANI, Ir. Alif Subardono, S.T., M.Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN JUDUL i
LEMBAR PENGESAHAN ii
PERNYATAAN KEASLIAN PROYEK AKHIR iii
KATA PENGANTAR iv
DAFTAR ISI vi
DAFTAR GAMBAR viii
DAFTAR TABEL x
DAFTAR LAMPIRAN xi
INTISARI xii
ABSTRACT xiii

BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 4
1.6 Sistematika Penulisan 4

BAB II TINJAUAN PUSTAKA DAN DASAR TEORI 5
2.1 Tinjauan Pustaka 5
2.2 Dasar Teori 9
2.2.1 *Security Information and Event Management* (*SIEM*) 9
2.2.2 *Open-Source Security Information Management (OSSIM)* 10
2.2.3 Splunk 11
2.2.4 VirtualBox 11
2.2.5 Linux 12
2.2.6 Debian 12
2.2.7 Kali Linux 12
2.2.8 *Web Server* 13
2.2.9 *Damn Vulnerable Web Application* (*DVWA*) 13
2.2.10 *SQL Injection* 13
2.2.11 *Cross-Site Scripting* (*XSS*) 14
2.2.12 *Directory Traversal* 15
2.2.13 *Port Scanning* 15
2.2.14 *Directory Brute Force* 15
2.3 Hipotesis 16

BAB III METODE PROYEK AKHIR 17
3.1 Alat dan Bahan 17
3.1.1 Spesifikasi Perangkat Keras (*Hardware*) 17
3.1.2 Spesifikasi Perangkat Lunak (*Software*) 17
3.2 Tahapan Penelitian 18

IMPLEMENTASI OSSIM DAN SPLUNK UNTUK MONITORING DAN ANALISA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
EMITA ARIANI, Ir. Alif Subardono, S.T., M.Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

3.3 Rancangan Sistem 21
3.3.1 Rancangan Topologi 21
3.3.2 Rancangan Arsitektur Sistem 22
3.4 Pengujian Sistem 24
3.4.1 Pengujian Fungsional 25
3.4.2 Pengujian Serangan 25

BAB IV HASIL PENELITIAN DAN PEMBAHASAN 33
4.1 Pengujian Fungsional 33
4.2 Pengujian Serangan Tunggal 35
4.2.1 Serangan *Directory Traversal* 35
4.2.2 Serangan *Cross-Site Scripting (XSS)* 37
4.2.3 Serangan *SQL Injection* 38
4.2.4 Serangan *Directory Brute Force* 41
4.2.5 Serangan *Port Scanning* 44
4.3 Pengujian Kombinasi 2 Serangan 46
4.4 Pengujian Kombinasi 3 Serangan 51
4.5 Pengujian Kombinasi 4 Serangan 57
4.6 Pengujian Kombinasi 5 Serangan 61

BAB V PENUTUP 64
5.1 Kesimpulan 64
5.2 Saran 65

DAFTAR PUSTAKA 66
LAMPIRAN 69